

Incidenten voorkomen door proactieve beveiliging

Predictive profiling, ook wel security profiling genoemd, is tot op de dag van vandaag enigszins beladen. Maar misschien is het wel de enige proactieve methode van beveiligen waarmee incidenten voorkomen kunnen worden. Voorwaarde is dan wel dat de security professional het systeem kan doorgronden, opzetten en onderhouden. Dit vraagt om kennis van de proactieve beveiligingscyclus. Als aan deze voorwaarde wordt voldaan, is deze beveiligingsbenadering ook goed bruikbaar binnen het zogenaamde drie-poorten-model. Het maakt dan niet meer uit of de tegenstander de organisatie probeert aan te vallen via de fysieke, personele of logische poort. Normafwijkingen en het signaleren van verdachte indicatoren zorgen er dan voor dat de aandacht in een vroegtijdig stadium wordt getrokken. In een stadium waarin nog preventief kan worden ingegrepen.

deel 1

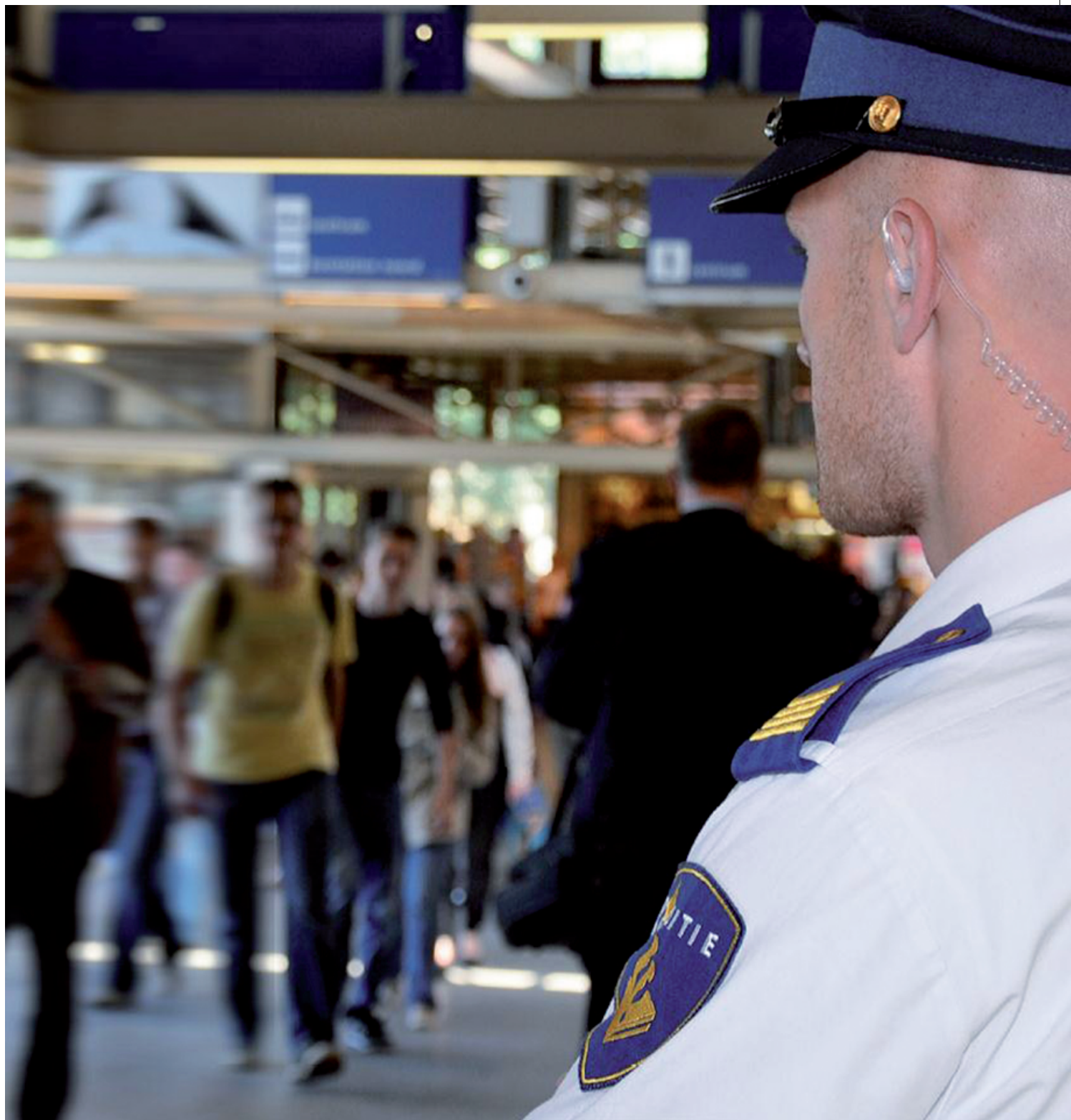
Management-summary

De basis voor predictive profiling is het zoeken naar afwijkingen in gedrag, houding of omgeving wat te koppelen is aan een onderkende criminele of terroristische methode van operatie, ook wel aanvallers methode van operatie (AMO) genoemd. Zelfs als een goede crimineel of terrorist iets doet wat niet mag, is er vrijwel altijd sprake van wat in de sociale en criminele wetenschappen 'lekkage' wordt genoemd. En juist de 'security profiler' is er op getraind om deze 'lekkage' waar te nemen in relatie tot de onderkende methode van operatie waarvan de aanvalleur gebruik maakt. Kennis van de acht stappen van de criminele en terroristische aanvalscyclus, ook wel criminele en terroristische planningcyclus genoemd, is daarbij onontbeerlijk.

De argwaan ten opzichte van predictive profiling komt grotendeels voort uit het niet begrijpen van het concept dat aan deze proactieve manier van beveiligen ten grondslag ligt. De belangrijkste misvatting is dat predictive profiling een synoniem is voor discriminatie, of erger, voor racisme. Niets is echter minder waar. Als de grondslag van predictive profiling daadwerkelijk een discriminerende of racistische blik op de wereld is, kan het concept niet werken. In een dergelijk geval hebben security professionals geen schijn van kans om criminaliteit of terrorisme te voorkomen. Hun blikveld zou dan te beperkt zijn. Een discriminerende of racistische grondslag betekent namelijk dat zij op zoek zijn naar mensen met een bepaalde huidskleur of manier van kleden. Met een dergelijk gekleurde bril naar de omgeving kijken heeft één zekerheid: datgene missen wat wij eigenlijk willen

waarnemen. De crimineel of terrorist waar wij naar op zoek zijn heeft namelijk geen bepaalde huidskleur of manier van kleden. Het kan iedereen zijn, ook onze meest integere en betrouwbare medewerker. Juist dit besef ligt aan het ontstaan van predictive profiling ten grondslag.

Concept De basis voor predictive profiling is het zoeken naar afwijkingen in gedrag, houding of omgeving wat te koppelen is aan een onderkende criminele of terroristische werkwijze, ook wel aanvallers methode van operatie (AMO) genoemd. Het zoeken naar afwijkingen kan op twee manieren plaatsvinden. Enerzijds kan gekeken worden of er zich situaties voordoen die afwijken van de norm of dat er gedragingen zijn die kunnen wijzen op 'kwade intentie'. In beide gevallen zal er wel een relatie met een AMO gelegd moeten kunnen worden. Dit betekent dat 'de norm' voor een bepaalde omgeving, situatie of tijd bekend



moet zijn en ook dat duidelijk moet zijn hoe mensen zich gedragen die kwaad in de zin hebben. Anderzijds kan door de security profiler actief worden gezocht naar indicatoren die kunnen wijzen op het manifest worden van een criminele of terroristische AMO. Dit betekent dat

staat moeten zijn om de waarneming te ontcrachten door het stellen van vragen. Daar waar de security profiler een plausibele verklaring kan vinden voor een waargenomen normafwijking of verdachte indicator wordt de mogelijke dreiging, het AMO voor een

personen of situaties die aan de security profiler voorbij komen niet worden gekeken. Zij kijken niet af van de norm en hebben geen verdachte indicatoren. Dit roept al gauw de vraag op of deze methode wel werkt? Een crimineel of terrorist kan toch opgaan in deze 99 procent van de mensen waar niet naar gekeken wordt?

De kracht van het concept security profiling is nu juist dat als er sprake is van voldoende kennis en alertheid bij de security profiler de crimineel en terrorist niet kan opgaan in de menigte. Eenvoudig omdat de crimineel of terrorist weet dat hij (of zij) iets doet wat niet mag en daardoor bepaalde signalen gaat uitzenden. Een goede ►

Predictive profiling is de enige proactieve beveiligingsmethode waarmee incidenten kunnen worden voorkomen.

de security profiler kennis moet hebben van AMO's in relatie tot de criminele en terroristische planningscyclus. Los van deze noodzakelijke kennis zal de security profiler vervolgens ook in

specifieke risicopositie, ontcracht. Dit zal veelal het resultaat zijn. Immers, in de meeste gevallen zal er niets aan de hand zijn. Bij een benadering zoals hier omschreven zal naar 99 procent van de



Het is daarbij wel belangrijk dat de security manager zich realiseert dat als er nieuwe AMO's getoetst worden, waarop medewerkers nog niet getraind zijn, het te verwachten is dat in de uitvoering er geen onderkenning van het AMO zal plaatsvinden. Niet erg, juist de bedoeling.

Serie In deze serie worden zowel de proactieve beveiligingscyclus, de criminele en terroristische plan-

crimineel of terrorist misschien minder dan een doorsnee mens die iets doet wat niet mag, maar er is altijd sprake van wat in de sociale en criminele wetenschappen 'lekkage' wordt genoemd. En juist de security profiler is er op getraind om deze 'lekkage' in relatie tot onderkende AMO's waar te nemen. Alleen een psychopaat, die vaak geen signalen zal lekken, kan onopgemerkt blijven.

Systeem Om het concept predictive profiling binnen een beveiligingsorganisatie te implementeren, zal een bewuste keuze moeten worden gemaakt om 'de proactieve beveiligingscyclus' te gaan implementeren. De zes stappen die onderdeel van deze cyclus zijn zullen, om de effectiviteit van de security profiler op de werkvloer te waarborgen, voortdurend opnieuw doorlopen moeten worden. De eerste stap in de cyclus is red teaming. Doel is het identificeren en testen op haalbaarheid van nieuwe AMO's. Het alleen uitgaan van incidenten uit het verleden is namelijk te beperkt. Onze tegenstanders ontwikkelen zich immers en worden steeds intelligenter. Dit betekent dat wij ook zelf, om een kans te hebben, actief op zoek moeten naar nieuwe manieren waarop onze organisatie te treffen is.

Na het identificeren van onze aanvallers methode van operatie zijn de vervolgstappen het identificeren van verdachte indicatoren, het ontwikkelen van standaard operationele procedures (SOP) voor de beveiligingsmedewerkers, het implementeren hiervan en het trainen van beveiligingsmedewerkers. Aan het einde van dit pro-actieve beveiligingsproces volgt weer red teaming. Na het voor de eerste keer hebben doorlopen van de gehele cyclus, krijgt red teaming twee doelstellingen. Het testen of de training van medewerkers adequaat is geweest en of verdachte indicatoren worden waargenomen. Daarnaast zal, zoals ook bij de eerste keer, worden gekeken of nieuwe AMO's gevonden kunnen worden.

ningscyclus alsook de toepassing van predictive profiling vanuit het drie-poorten-model verder uitgewerkt. In juni wordt stil gestaan bij de criminele en terroristische planningscyclus. Daarna wordt in september het begrip 'red teaming' uitgewerkt. Dit is de eerste stap van de proactieve beveiligingscyclus. Daarna wordt in december stilgestaan bij stap 2 van de proactieve beveiligingscyclus (bepalen AMO), in maart 2014 bij stap 3 (vaststellen verdachte indicatoren), in juni 2014 bij stap 4 (ontwikkelen SOP), in september 2014 bij stap 5 (implementatie SOP) en in december 2014 bij de laatste en zesde stap van de proactieve beveiligingscyclus: het trainen van medewerkers. Vervolgens wordt in maart 2015 de toepassing van de proactieve beveiligingsbenadering vanuit het drie-poorten-model uitgewerkt. Na dit laatste artikel in deze serie weet u als security professional hoe de methodiek te gebruiken is voor fysieke beveiliging (fysieke poort), voor pre-employment en in-employment screening (personele poort) alsook binnen de IT-security (logische poort).

Opleidingen Zowel SoSecure als de Orca Secure Academy organiseren, in samenwerking met de European Security Intelligence Foundation, regelmatig opleidingen op het vlak van predictive profiling. Het afsluiten van deze opleiding is de eerste stap naar de inschrijving in het register 'Certified Security Profiler' van de Stichting N'Lloyd. Binnen de genoemde opleidingen worden de benodigde handvaten aangereikt om de methodiek van het proactief beveiligen succesvol binnen uw organisatie te implementeren. De docenten die aan deze cursussen verbonden zijn hebben in Nederland inmiddels allemaal hun sporen achtergelaten in het relatief nieuwe vakgebied van predictive profiling.

■ Berndt Rif MSc MBA MSec, Berndt.Rif@beveiliging.nl
Marie Louise Ruijs BPM, MarieLouise.Ruijs@promundo.nl